Solving linear equations over finitely generated abelian groups

René Hartung

July 16, 2010

Abstract

We discuss various methods and their effectiveness for solving linear equations over finitely generated abelian groups. More precisely, if $\varphi\colon G \to H$ is a homomorphism of finitely generated abelian groups and $b \in H$, we discuss various algorithms for checking whether or not $b \in \mathrm{im}\varphi$ holds and if so, for computing a pre-image of b in G together with the kernel of φ.

1 Introduction

Solving linear equations over finitely generated abelian groups is an important tool for computing $H^2(G, A)$ of a given G-module A. Therefore algorithms for solving linear equations are important in extension theory of groups, see Section 8.7 of [6]. For extending the Small Groups Library, see e.g. [1], we need effective algorithms especially for this problem. In this note, we discuss various methods and we propose an effective algorithm which performs well on a broad range of randomly chosen linear equations.

2 Preliminaries

Let G and H be finitely generated abelian groups and let $\varphi\colon G \to H$ be a homomorphism. Further let $b \in H$ be given. A *linear equation over* G asks whether or not $b \in \mathrm{im}\varphi$ holds and, if so, for computing a pre-image of b in G together with the kernel of φ.

3 Standard methods for polycyclic groups

Since the groups G and H are finitely generated and abelian, both are polycyclic. Therefore the methods for homomorphisms of polycyclic groups described in [2, Section 3.5.2] apply. We briefly summarize these methods here for completeness.

The homomorphism $\varphi\colon G \to H$ naturally corresponds to the subgroup $U_\varphi = \{(g^\varphi, g) \mid g \in G\}$ of the direct product $H \times G$. Given polycyclic sequences $\mathcal{G}$ and $\mathcal{H}$ of G and H respectively, the algorithms in [2] allow to compute an induced polycyclic sequence for U_φ with respect to $\mathcal{H} \times \mathcal{G}$. This sequence allows to read off the kernel of φ and can be used to decide whether or not $b \in \mathrm{im}\varphi$ holds.

Lemma 1 (Eick, 2001) *Let φ be a group homomorphism and $\mathcal{U}$ be an induced polycyclic sequence for U_φ with respect to $\mathcal{H} \times \mathcal{G}$. Then $\mathcal{U}$ has the form $((\bar{u}_1, u_1), \ldots, (\bar{u}_s, u_s))$ with $u_i \in G$ and $\bar{u}_i \in H$. Let t be maximal with $\bar{u}_t \neq 1$.*

(A) *Then $(\bar{u}_1, \ldots, \bar{u}_t)$ is an induced polycyclic sequence for the image of φ with respect to $\mathcal{H}$.*

(B) *Then $(u_{t+1}, \ldots, u_s)$ is an induced polycyclic sequence for the kernel of φ with respect to $\mathcal{G}$.*

Proof. For a proof, we refer to [2, p.36]. □

This method is implemented in the POLYCYCLIC package of GAP, see [3]. However, for finitely generated abelian groups, we can do much better as we will show in the following.

4 Solution by solving linear Diophantine equations

In this section we describe a more effective algorithm relying on linear algebra only. Let G be a finitely generated abelian group. Then G decomposes into its torsion subgroup $T(G)$ and a free abelian subgroup so that $G \cong \mathbb{Z}^\ell \times T(G)$ holds. Further, the torsion subgroup $T(G)$ decomposes into its p-Sylow subgroups so that we may identify

$$G = \mathbb{Z}^\ell \oplus \mathrm{Syl}_{p_1}(T(G)) \oplus \cdots \oplus \mathrm{Syl}_{p_k}(T(G)),$$

where $\mathrm{Syl}_{p_i}(T(G))$ denotes the p_i-Sylow subgroup of $T(G)$. Similarly, we can identity

$$H = \mathbb{Z}^{\ell'} \oplus \mathrm{Syl}_{p_1}(T(H)) \oplus \cdots \oplus \mathrm{Syl}_{p_k}(T(H)).$$

Every homomorphism $\varphi\colon G \to H$ induces a homomorphism $\varphi_i = \varphi|_{\mathrm{Syl}_{p_i}(T(G))}$ of the p_i-Sylow subgroup. Assume that $\mathrm{Syl}_{p_i}(T(H)) \cong \mathbb{Z}_{p_i^{\alpha_{i1}}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{\alpha_{in_i}}}$ holds. Then, with respect to an independent generating set of G, the equation $x^\varphi = b$ translates to equations of the form

$$\begin{pmatrix} A_t & B \\ 0 & A_s \end{pmatrix} \xi = \beta \pmod{[p_1^{\alpha_{11}}, \ldots, p_m^{\alpha_{mn_m}}, 0, \ldots, 0]} \tag{1}$$

where $a_{i1}x_1 + \cdots + a_{in}x_n = b_i \pmod 0$ denotes the Diophantine equation, the sub-matrix A_t is a block diagonal matrix describing the homomorphisms $\varphi_1, \ldots, \varphi_k$, while A_s incorporates the action of φ on the free abelian subgroup $\mathbb{Z}^\ell \cong G/T(G)$.

For solving (1), we introduce free variables, one for each generator of the torsion subgroup $T(G)$. Thereby we obtain a linear system of Diophantine equations of the form

$$\begin{pmatrix} A_t & B & D \\ 0 & A_s & 0 \end{pmatrix} \hat{\xi} = \beta \tag{2}$$

where $D = \mathrm{diag}(p_1^{\alpha_{11}}, \ldots, p^{\alpha_{mn_m}})$ is a diagonal matrix describing the modular equations of the form $a_{i1}x_1 + \cdots + a_{i\ell}x_\ell \equiv b_i \pmod{p^{\alpha_{ij}}}$.

4.1 Solving linear Diophantine equations

The linear system of Diophantine equations in (2) can be solved using the Smith normal form; see [7]. Recall that, for every $A \in \mathbb{Z}^{m\times n}$ there are unimodular matrices $L \in \mathrm{SL}(m,\mathbb{Z})$ and $R \in \mathrm{SL}(n,\mathbb{Z})$ such that LAR is a diagonal matrix $D = \mathrm{diag}(d_1,\dots,d_r,0,\dots,0)$ whose non-zero entries $d_1,\dots,d_r$ satisfy $d_i \mid d_{i+1}$ for every $i < r = \mathrm{rk}(A)$.

Therefore the linear system $Ax = b$ of linear Diophantine equations in (2) is equivalent to the equations $Dy = Lb$ and $x = Ry$. Write $c = Lb$. Then the system $Dy = c$ has an integral solution if and only if $d_i \mid c_i$ holds for every $1 \le i \le r$ and $c_i = 0$ otherwise. If the equation $Dy = c$ has an integral solution, then these are given by $y = (c_1/d_1,\dots,c_r/d_r,t_1,\dots,t_{n-r})$ with $t_1,\dots,t_{n-r} \in \mathbb{Z}$. Every solution x to the linear system of Diophantine equations $Ax = b$ is then easily obtained as $x = Ry$.

It is well known, [5], that computing the Smith normal form of an integral matrix is computationally hard due to the unavoidable growth of the intermediate matrix entries. Even though there are improvements in special cases, see or [6, Section 9.3] for an overview, we cannot expect the algorithm in this section to be practical in general. Especially for groups with a large torsion-subgroup, the problem grows significantly by forming the system of linear Diophantine equations in (2). Therefore reducing to a minimal generating set for the torsion subgroup first might improve this algorithm. Note that especially finite groups are a problem here.

We can use a different and more effective approach for finitely generated abelian groups which first considers the linear system of Diophantine equations arising from the torsion-free part in G and H. Afterwards, our approach solves the equations over the torsion subgroups with varying the right-hand-sides with respect to the solutions of the torsion-free part.

5 Solving linear equations over finite abelian groups

In the remainder we consider linear equations over finite abelian groups only. Let G and H be finite abelian groups. Suppose that $p_1,\dots,p_n$ are prime numbers such that $|G| = p_1^{e_1}\cdots p_n^{e_n}$ and $|H| = p_1^{f_1}\cdots p_n^{f_n}$ with $e_i, f_i \in \mathbb{N}\cup\{0\}$. Since every homomorphism $\varphi\colon G \to H$ induces a homomorphism $\varphi_i\colon \mathrm{Syl}_{p_i}(G) \to \mathrm{Syl}_{p_i}(H)$ of the p_i-Sylow subgroups, we may restrict to the case that G and H are abelian p-groups. More precisely, if we identify

$$G = \mathrm{Syl}_{p_1}(G) \times \cdots \times \mathrm{Syl}_{p_n}(G) \quad \text{and} \quad H = \mathrm{Syl}_{p_1}(G) \times \cdots \times \mathrm{Syl}_{p_n}(G),$$

then we can decompose φ into homomorphisms $\varphi_i\colon \mathrm{Syl}_{p_i}(G) \to \mathrm{Syl}_{p_i}(H)$ with $\varphi|_{\mathrm{Syl}_{p_i}(G)} = \varphi_i$. This yields that φ decomposes as $\varphi_1\times\cdots\times\varphi_n$, where $\varphi_1\times\cdots\times\varphi_n$ acts diagonally by

$$(g_1,\dots,g_n)^{\varphi_1\times\cdots\times\varphi_n} = (g_1^{\varphi_1},\dots,g_n^{\varphi_n}).$$

Computing pre-images and the kernel of φ can be done independently for the p_i-Sylow subgroups. In particular, solving linear equations over finite abelian groups split into independent computations for the Sylows subgroups and hence, can easily be parallelized.

6 Solving linear equations over abelian p-groups

Let G and H be abelian p-groups and let $\varphi\colon G \to H$ be a homomorphism. We identify $G = \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_n}}$ and $H = \mathbb{Z}_{p^{f_1}} \times \cdots \times \mathbb{Z}_{p^{f_m}}$ with $e_1 \leq \ldots \leq e_n$ and $f_1 \leq \ldots \leq f_m$. Further let $\{g_1, \ldots, g_n\}$ and $\{h_1, \ldots, h_m\}$ be independent generating sets of G and H with $|g_i| = p^{e_i}$ and $|h_i| = p^{f_i}$, respectively. Then we can represent φ by an m-by-n matrix $A = (a_{ij})_{i,j}$ where $(a_{1j}, \ldots, a_{mj}) = (\alpha_1, \ldots, \alpha_m)$ whenever $g_j^{\varphi} = h_1^{\alpha_1} \cdots h_m^{\alpha_m}$ holds.

Computing a pre-image of $b = h_1^{b_1} \cdots h_m^{b_m} \in H$ together with the kernel of φ is equivalent to solving the linear system of modular equations

$$\begin{array}{ccccccccc} a_{11}x_1 & + & \cdots & + & a_{1n}x_n & \equiv & b_1 & \pmod{p^{f_1}} \\ \vdots & & \ddots & & \vdots & \vdots & & \vdots \\ a_{m1}x_1 & + & \cdots & + & a_{mn}x_n & \equiv & b_m & \pmod{p^{f_m}} \end{array} \tag{3}$$

We discuss the following methods for solving (3):

(A) solving a linear system of Diophantine equations,

(B) using the method for polycyclic groups described in [2],

(C) using a modular analog of Smith normal form in the case that G and H are both homocyclic,

(D) using the method in (C) and lifting solutions recursively,

(E) lifting a solution over $\mathbb{F}_p$ recursively with the Hensel lemma.

In Section **??** we show the application of these algorithms to various randomly chosen equations.

6.1 Solving linear equations over homocyclic p-groups

Let G and H be homocyclic p-groups; that is, $G \cong \mathbb{Z}_{p^\ell} \times \cdots \times \mathbb{Z}_{p^\ell}$ for some k copies of $\mathbb{Z}_{p^\ell}$. We generalize the algorithm of Section 4 to solve linear equations over homocyclic groups.

Let $\varphi\colon G \to H$ be a homomorphism and let $g \in H$ be given. Then the endomorphism φ is represented by an m-by-n matrix $A = (a_{ij})_{i,j}$ while $g \in H$ translates to its corresponding exponent vector $(b_1, \ldots, b_m)$. For computing all solutions to the system $Ax \equiv b \pmod{p^\ell}$, we use the following modular analog of the Smith normal form:

Lemma 2 *Let $A \in (\mathbb{Z}_{p^\ell})^{m\times n}$ be given. Then there exist matrices $L \in (\mathbb{Z}_{p^\ell})^{m\times m}$ and $R \in (\mathbb{Z}_{p^\ell})^{n\times n}$, which are invertible modulo p^ℓ, so that LAR is a diagonal matrix $D = \operatorname{diag}(d_1, \ldots, d_k, 0, \ldots, 0)$ whose non-zero entries $d_1, \ldots, d_k$ satisfy $d_i \mid d_{i+1}$ for each $1 \leq i < k$.*

Proof. We give a constructive proof for this lemma. For a positive integer $n = a \cdot p^\ell$ with $\gcd(a,p) = 1$, we denote by $\nu_p(n) = \ell$ the *p-evaluation of n*. Choose indices $1 \le i \le m$ and $1 \le j \le n$ so that

$$\nu_p(a_{ij}) = \min\{\nu_p(a_{\iota\kappa}) \mid 1 \le \iota \le m, 1 \le \kappa \le n\}$$

By permuting the rows and columns of A, we may assume that $a_{ij} = a_{11}$ holds. Then $a_{11} = a \cdot p^{\nu_p(a_{11})}$ for some integer a with $\gcd(a,p) = 1$. In particular, the integer a is invertible modulo p^ℓ. Multiplying the first row by the inverse α of a yields that the entries a_{i1}, with $2 \le i \le m$, are all divisible by $\alpha a_{11} \equiv p^{\nu_p(a_{11})} \pmod{p^\ell}$. Similarly, the entries αa_{1j}, with $2 \le j \le n$, are all divisible by αa_{11}. Therefore, we can find matrices L_1 and R_1 so that

$$L_1 A R_1 = \begin{pmatrix} p^{\nu_p(a_{11})} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \tilde{A} & \\ 0 & & & \end{pmatrix}$$

holds. Continuing with the $(m-1) \times (n-1)$ sub-matrix $\tilde{A}$ recursively would finally yield matrices L and R so that $LAR = D$ is diagonal. A permutation of the rows and columns of D would then give the divisibility claimed above. □

The algorithm of Section 4 now readily generalizes to an algorithm for solving the linear equation $Ax \equiv b \pmod{p^\ell}$: By Lemma 2, there exist matrices L and R so that

$$LAR = \mathrm{diag}(d_1, \ldots, d_k, 0, \ldots, 0).$$

Therefore the linear equation $Ax \equiv b \pmod{p^\ell}$ translates to the systems $Dy \equiv Lb \pmod{p^\ell}$ and $x \equiv Ry \pmod{p^\ell}$. It remains to check whether or not the diagonal system $Dy \equiv Lb \pmod{p^\ell}$ has a solution and, if so, to determine all these solutions. This is a straightforward application of elementary number theory.

Clearly for solving the linear system $Ax \equiv b \pmod{p^\ell}$ the explicit computation of L is not necessary. Instead we can apply the row operations directly to the right-hand-side b which is cheaper in general.

6.2 Solving linear equations using the block structure

The algorithm of Section 6.1 generalizes to a method for solving a linear system of equations over arbitrary abelian p-groups as we will describe in the following.

Let G and H be arbitrary abelian p-groups. Further let $\varphi\colon G \to H$ be a homomorphism and let $g \in H$ be given. We decompose the groups G and H into direct products

$$G = (\mathbb{Z}_{p^{e_1}})^{g_1} \times \cdots \times (\mathbb{Z}_{p^{e_\ell}})^{g_\ell} \quad \text{and} \quad H = (\mathbb{Z}_{p^{e_1}})^{h_1} \times \cdots \times (\mathbb{Z}_{p^{e_\ell}})^{h_\ell}$$

with $e_1 < \ldots < e_\ell$ and $g_i, h_i \in \mathbb{N} \cup \{0\}$. Clearly, in the descending chains of subgroups

$$G \ge p^{e_1} G \ge \ldots \ge p^{e_\ell} G = \{0\} \quad \text{and} \quad H \ge p^{e_1} G \ge \ldots \ge p^{e_\ell} H = \{0\}.$$

the factors $p^{e_i}G/p^{e_{i+1}}G$ and $p^{e_i}H/p^{e_{i+1}}H$ are homocyclic of rank $g_{i+1}+\cdots+g_\ell$ and $h_{i+1}+\cdots+h_\ell$, respectively. Every homomorphism $\varphi\colon G\to H$ maps the subgroup $p^{e_i}G$ to $p^{e_i}H$ and therefore induces a homomorphism $\varphi^{(i)}\colon G/p^{e_{i+1}}G \to H/p^{e_{i+1}}H$ Let ι_i, δ_i, κ_i, and ε_i denote the natural homomorphisms so that the diagram

$$\begin{tikzcd}
G \arrow[rrr, bend left, "\varphi"] \arrow[dr, "\iota_{i+1}"] \arrow[ddr, bend right, "\iota_i"'] & & & H \arrow[dl, "\kappa_{i+1}"'] \arrow[ddl, bend left, "\kappa_i"] \\
& G/p^{e_{i+1}}G \arrow[r, "\varphi^{(i+1)}"] \arrow[d, "\delta_i"] & H/p^{e_{i+1}}H \arrow[d, "\varepsilon_i"] & \\
& G/p^{e_i}G \arrow[r, "\varphi^{(i)}"] & H/p^{e_i}H &
\end{tikzcd}$$

commutes. Since the quotients $G/p^{e_1}G$ and $H/p^{e_1}H$ are both homocyclic, the algorithm of Section 6.1 computes an $x_1\in G$ so that $x_1^\varphi - b\in\ker\kappa_1$ holds together with a generating set for some $K_1\subseteq G$ with $K_1^{\iota_1}=\ker\varphi^{(1)}$. In the remainder of this section, we lift these solutions recursively to a solution of $x^\varphi=b$. The following lemma lifts the special solution x_i.

Lemma 3 *The solution x_i lifts to a solution x_{i+1} if and only if there exists $\lambda\in G$ such that $\lambda^{\iota_i}\in\ker\varphi^{(i)}$ with $x_{i+1}=x_i-\lambda$ and*

$$(x_i^\varphi - b)^{\kappa_{i+1}} = \lambda^{\varphi\kappa_{i+1}} = \lambda^{\iota_{i+1}\varphi^{(i+1)}}. \tag{4}$$

Proof. Let $\lambda\in G$ be as above. Then

$$(x_{i+1}^\varphi - b)^{\kappa_{i+1}} = ((x_i-\lambda)^\varphi - b)^{\kappa_{i+1}} = x_i^{\varphi\kappa_{i+1}} - \lambda^{\varphi\kappa_{i+1}} - b^{\kappa_{i+1}} = 0,$$

and hence $x_{i+1}^\varphi - b$ lifts the solution x_i. Assume that the solution x_i lifts to the solution x_{i+1}; that is, we both have $x_{i+1}^\varphi - b\in\ker\kappa_{i+1}$ and $x_i^\varphi - b\in\ker\kappa_i$. Recall that $\ker\kappa_i = p^{e_i}H \geq p^{e_{i+1}}H = \ker\kappa_{i+1}$. This yields that $(x_{i+1}-x_i)^\varphi\in\ker\kappa_i$ and hence

$$0 = (x_{i+1}-x_i)^{\varphi\kappa_i} = (x_{i+1}-x_i)^{\iota_i\varphi^{(i)}}.$$

Therefore $(x_{i+1}-x_i)^{\iota_i}\in\ker\varphi^{(i)}$. □

It remains to lift the kernel of the linear equation. Let $K_i\subseteq G$ be a pre-image of $\ker\varphi^{(i)}$ in G. Then a generating set for K_i is easily obtained from the generating sets of $\ker\varphi^{(i)}$ and $\ker\iota_i$. Suppose that $K_i=\langle k_1,\ldots,k_\ell\rangle$ holds. Since we have that $\iota_i\varphi^{(i)}=\varphi\kappa_i$, it follows that

$$K_i^{\varphi\kappa_{i+1}} = K_i^{\iota_{i+1}\varphi^{(i+1)}} \leq \ker\varepsilon_i = p^{e_i}H/p^{e_{i+1}}H.$$

It suffices to check whether or not $x_i^\varphi - b\in\langle k_1^{\varphi\kappa_{i+1}},\ldots,k_\ell^{\varphi\kappa_{i+1}}\rangle$ holds. Since $K_i^{\varphi\kappa_{i+1}}\leq p^{e_i}H/p^{e_{i+1}}H$, the latter condition is equivalent to solve an equation over the homocyclic group $p^{e_i}H/p^{e_{i+1}}H$. A solution to this latter system yields a lift of the solution x_i as described in Lemma 3. Furthermore, the following lemma outlines the lift of K_i to K_{i+1}.

Lemma 4 *Let $K_i \leq G$ be given so that $K_i^{\iota_i} = \ker \varphi^{(i)}$ holds. Then it holds that*

$$K_{i+1} = \langle \{k \in K_i \mid k^{\varphi\kappa_{i+1}} = 0\} \cup \{p^{e_{i+1}-e_i}\, k \mid k \in K_i\} \rangle.$$

Proof. Let $k \in K_i$ be so that $k^{\varphi\kappa_{i+1}} = 0$. Then, as $\varphi\kappa_{i+1} = \iota_{i+1}\varphi^{(i+1)}$, it holds that $k^{\iota_{i+1}\varphi^{(i+1)}} = 0$ and therefore, $k^{\iota_{i+1}} \in \ker \varphi^{(i+1)}$. Write $\Delta p = p^{e_{i+1}-e_i}$ and let $k \in K_i$ be given. Then it follows that

$$(\Delta p\, k)^{\iota_{i+1}\varphi^{(i+1)}} = (\Delta p\, k)^{\varphi\kappa_{i+1}}$$

and, since $k^\varphi \in p^{e_i} H = \ker \kappa_i$, we also have that

$$(\Delta p\, k)^\varphi = \Delta p\, k^\varphi \in p^{e_{i+1}} H = \ker \kappa_{i+1}.$$

This yields that $L = \Delta p\, K_i$ is contained in K_{i+1} and, as $k^\varphi \in \ker \kappa_{i+1} \leq \ker \kappa_i$, it follows that $K_{i+1} \leq K_i$. Hence, every element $g \in K_{i+1} \setminus L$ can be written as $g = ab$ with $b \in L$ and $a \in K_{i+1}$ with $aL \neq L$. Then we get

$$0 = g^{\iota_{i+1}\varphi^{(i+1)}} = (ab)^{\varphi\kappa_{i+1}} = a^{\varphi\kappa_{i+1}}\, b^{\varphi\kappa_{i+1}}$$

where $b^{\varphi\kappa_{i+1}} = 0$. Hence the element $a \in K_i$ satisfies $a^{\varphi\kappa_{i+1}} = 0$. □

Note that the generating set of K_{i+1} defined in Lemma 4 may contain redundancies. These significantly affect the complexity of the algorithm in Section 6.1.

6.3 On a number theoretical approach

In this section we describe a number theoretical approach which avoids the redundancies introduced in the lifting of the kernels in Section 6.2. Our overall strategy for solving (1) is an induction on the exponents $f_1, \ldots, f_m$. More precisely, we solve the linear system $Ax \equiv b \pmod p$ over the finite field $\mathbb{F}_p$ with Gaussian elimination. Then we lift the obtained solutions recursively by applying the Hensel lemma. First we only consider an abelian p-group G and an endomorphism $\varphi\colon G \to G$.

6.3.1 Solving endomorphic equations over finite p-groups

Let G be a finite p-group and let $\varphi\colon G \to G$ be an endomorphism. Further let $b \in G$ be given. We describe an algorithm for solving the linear equation $x^\varphi = b$ or, equivalently, the linear system of modular equations

$$\begin{array}{ccccccc} a_{11}x_1 & + & \cdots & + & a_{1m}x_m & \equiv & b_1 \pmod{p^{e_1}} \\ \vdots & & \ddots & & \vdots & & \vdots \\ a_{m1}x_1 & + & \cdots & + & a_{mm}x_m & \equiv & b_m \pmod{p^{e_m}}. \end{array} \tag{5}$$

Note that the matrix $A = (a_{ij})_{1\leq i,j\leq m}$ in (5) satisfies the condition

$$p^{e_i - e_{\min\{i,j\}}} \mid a_{ij} \qquad \text{for each } 1 \leq i, j \leq m, \tag{6}$$

as it corresponds to the endomorphism φ; see also [8]. Denote the linear system of equations in (5) by $Ax \equiv b \pmod{[p^{e_1}, \ldots, p^{e_m}]}$.

Clearly, using Gaussian elimination, we can find all solutions to the linear system $Ax \equiv b \pmod{[p, \ldots, p]}$ efficiently. Every solution $x = (x_1, \ldots, x_m)$ to the system over the finite fields $\mathbb{F}_p$ has the form $x = \xi_0 + \xi_1 t_1 + \cdots + \xi_r t_r$ where, for each $1 \le i \le r$, it holds that $A\xi_i \equiv 0 \pmod{[p, \ldots, p]}$ and $t_i \in \{0, \ldots, p-1\}$.

The overall idea for solving (5) is to lift these solutions simultaneously by keeping the coefficients $t_1, \ldots, t_r$ in the finite field $\mathbb{F}_p$. This yields that, if $|\ker \varphi| = p^r$, we obtain r independent homogeneous solutions $\xi_1, \ldots, \xi_r$. For $\ell \in \{1, \ldots, e_m\}$ and $k = \min\{i \mid \ell \le e_i\}$, we assume that all solutions to the linear system $Ax \equiv b \pmod{[p^{e_1}, \ldots, p^{e_{k-1}}, p^\ell, \ldots, p^\ell]}$ are given by

$$x = \xi_0 + t_1\xi_1 + \cdots + t_r\xi_r, \tag{7}$$

where $t_i \in \{0, \ldots, p-1\}$ for each $1 \le i \le r$. Applying the Hensel lemma, we lift the solutions in (7) to solutions to $Ax \equiv b \pmod{[p^{e_1}, \ldots, p^{e_{k-1}}, p^{\ell+1}, \ldots, p^{\ell+1}]}$. For this purpose, we consider the modular equations

$$\begin{array}{ccccccccc} a_{k1}x_1 & + & \cdots & + & a_{km}x_m & \equiv & b_k & \pmod{p^{\ell+1}} \\ \vdots & & \ddots & & \vdots & & & \vdots \\ a_{m1}x_1 & + & \cdots & + & a_{mm}x_m & \equiv & b_m & \pmod{p^{\ell+1}}. \end{array}$$

By condition (6), the solutions $x_i \pmod{p^{e_i}}$, for each $1 \le i < k$, do not need to be considered anymore. Similar to Section 6.1, we can find a matrix $L \in \mathbb{Z}^{m \times m}$, which is invertible modulo $p^{\ell+1}$, so that $\tilde{A} = LA$ is the matrix of an equivalent system of modular equations so that $\tilde{A} = (\tilde{a}_{ij})_{k \le i \le m, 1 \le j \le m}$ still satisfies

$$p^{e_i - e_{\min\{i,j\}}} \mid \tilde{a}_{ij} \quad \text{for each } k \le i \le m \text{ and } 1 \le j < k,$$

and the sub-matrix $(\tilde{a}_{ij})_{k \le i,j \le m}$ is upper-triangular. Assume that all solutions to $Ax \equiv b \pmod{[p^{e_1}, \ldots, p^{e_{k-1}}, p^\ell, \ldots, p^\ell, p^{\ell+1}, \ldots, p^{\ell+1}]}$ are given *uniquely* by

$$x = \xi_0 + t_1\xi_1 + \cdots + t_r\xi_r \tag{8}$$

with $t_i \in \{0, \ldots, p-1\}$; that is, the solutions $x_m, x_{m-1}, \ldots, x_{n-1}$ modulo p^ℓ are already lifted to solutions modulo $p^{\ell+1}$. We show how to lift the solutions $x_n = x_n(t_1, \ldots, t_r)$ modulo p^ℓ modulo $p^{\ell+1}$. Consider the modular equation

$$a_{l1}x_1 + \cdots + a_{lk}x_k + a_{ln}x_n + \cdots + a_{lm}x_m \equiv b_l \pmod{p^{\ell+1}}$$

for some $k \le l \le m$. This equation can be considered a polynomial $\tilde{f} \in \mathbb{Z}[x_n]$ with zeros modulo p^ℓ given by $x_n = x_n(t_1, \ldots, t_r)$ for any choice of $t_1, \ldots, t_r \in \{0, \ldots, p-1\}$. More precisely, we define $\tilde{f}(x_n) = f(x_n) - b_l$ where

$$f(x_n) = a_{l1}x_1 + \cdots + a_{lk}x_k + a_{ln}x_n + \cdots + a_{lm}x_m.$$

The Hensel lemma now applies to the polynomial $\tilde{f}$ and its zeros $x_n(t_1, \ldots, t_r)$: Let $\tilde{f}'(x_n) = \tilde{a}_{ln}$ denote the formal derivation of $\tilde{f}$. Using the linearity of the polynomial f, we obtain the following lemma which gives a condition for a unique lift of the zeros $x_n = x_n(t_1, \ldots, t_r)$.

Lemma 5 *If $\tilde{f}'(x_n) \not\equiv 0 \pmod p$ holds, then the solutions $x_n = x_n(t_1, \ldots, t_r)$ lift uniquely to $x_n + t \cdot p^\ell$ where $t \in \{0, \ldots, p-1\}$ is given by*

$$t \quad \equiv \quad -(\tilde{a}_{ln})^{-1} \left(\frac{f(\xi_0) - b_h}{p^\ell} + \frac{f(\xi_1)}{p^\ell} t_1 + \cdots + \frac{f(\xi_r)}{p^\ell} t_r \right) \pmod p. \quad (9)$$

Proof. The proof follows immediately from the Hensel lemma. □

Recall that a solution $x_n(t_1, \ldots, t_r)$ modulo p^ℓ may not lift to a solution modulo $p^{\ell+1}$. The following lemma gives a sufficient and necessary condition for such a lift.

Lemma 6 *If $\tilde{f}'(x_n) \equiv 0 \pmod p$ holds, then the solutions $x_n = x_n(t_1, \ldots, t_r)$ lift if and only if the coefficients $t_1, \ldots, t_r \in \{0, \ldots, p-1\}$ satisfy*

$$\frac{f(\xi_0) - b_h}{p^\ell} + \frac{f(\xi_1)}{p^\ell} t_1 + \cdots + \frac{f(\xi_r)}{p^\ell} t_r \equiv 0 \pmod p. \quad (10)$$

If this is the case, then the solutions $x_n = x_n(t_1, \ldots, t_r)$ lift to $x_n + t_{r+1} p^\ell$ for each $t_{r+1} \in \{0, \ldots, p-1\}$.

Proof. The proof follows immediately from the Hensel lemma. □

The linearity of (10) allows to eliminate a free variable t_s, say, if this equation is not trivially satisfied; that is, at least one coefficient does not vanish modulo p. More precisely, writing $\gamma_i = f(\xi_i)/p^\ell$, for each $1 \le i \le r$, and $\gamma_0 = (f(\xi_0) - b)/p^\ell$, we may have that $f(\xi_s) \not\equiv 0 \pmod{p^{\ell+1}}$ but $f(\xi_{s+1}) \equiv \ldots \equiv f(\xi_r) \equiv 0 \pmod{p^{\ell+1}}$. Then we may restrict

$$t_s \equiv -\gamma_s^{-1} (\gamma_0 + \gamma_1 t_1 + \cdots + \gamma_{s-1} t_{s-1}) \pmod p. \quad (11)$$

The following lemma determines an independent subset of solutions of (8) which lift by Lemma 6.

Lemma 7 *If $f(\xi_s) \not\equiv 0 \pmod{p^{\ell+1}}$ holds while $f(\xi_{s+1}) \equiv \ldots \equiv f(\xi_r) \equiv 0 \pmod{p^{\ell+1}}$, then the combinations of the elements*

$$\tilde{\xi}_i = \begin{cases} \xi_i - \gamma_s^{-1} \gamma_i \xi_s, & \textit{for each } 1 \le i \le s-1 \\ \xi_i, & \textit{for each } s+1 \le i \le r. \end{cases} \quad (12)$$

are p^{r-1} solutions amongst (8) which satisfy $f(x_n) \equiv 0 \pmod{p^{\ell+1}}$.

Proof. It is easy to see that for any element $\tilde{\xi}_i$ in (12) it holds that $f(x_n) \equiv 0 \pmod{p^{\ell+1}}$. Thus it remains to prove that these elements are independent modulo $[p^{e_1}, \ldots, p^{e_k}, p^\ell, \ldots, p^{\ell+1}, p^{\ell+1}, \ldots, p^{\ell+1}]$. For this purpose, assume that we are given $t_i, u_i \in \{0, \ldots, p-1\}$ such that

$$\tilde{\xi}_0 + \sum_{i \ne s} t_i \tilde{\xi}_i \equiv \tilde{\xi}_0 + \sum_{i \ne s} u_i \tilde{\xi}_i \pmod{[\ldots, p^{\ell+1}, \ldots]}$$

holds. Then, by construction, we have that

$$\begin{aligned} & \xi_0 + \sum_{i \neq s} t_i \xi_i - \gamma_s^{-1}(\gamma_0 + \gamma_1 t_1 + \cdots + \gamma_{s-1} t_{s-1}) \xi_s \\ \equiv \quad & \xi_0 + \sum_{i \neq s} u_i \xi_i - \gamma_s^{-1}(\gamma_0 + \gamma_1 u_1 + \cdots + \gamma_{s-1} u_{s-1}) \xi_s \pmod{[\ldots, p^{\ell+1}, \ldots]} \end{aligned}$$

By Equation (11), there exist $\delta, \varepsilon \in \mathbb{Z}$ so that

$$\begin{aligned} t_s &= -\gamma_s^{-1}(\gamma_0 + \gamma_1 t_1 + \cdots + \gamma_{s-1} t_{s-1}) + \delta p \\ u_s &= -\gamma_s^{-1}(\gamma_0 + \gamma_1 u_1 + \cdots + \gamma_{s-1} u_{s-1}) + \varepsilon p. \end{aligned} \tag{13}$$

Thus we obtain that

$$\xi_0 + \sum_{i=1}^{r} t_i \xi_i + \delta p \xi_s \equiv \xi_0 + \sum_{i=1}^{r} u_i \xi_i + \varepsilon p \xi_s \pmod{[\ldots, p^{\ell+1}, \ldots]}.$$

and, in particular,

$$\xi_0 + \sum_{i=1}^{r} t_i \xi_i + \delta p \xi_s \equiv \xi_0 + \sum_{i=1}^{r} u_i \xi_i + \varepsilon p \xi_s \pmod{[\ldots, p^{\ell}, \ldots]}. \tag{14}$$

If $p\xi_s$ vanishes modulo $[\ldots, p^\ell, \ldots]$, the claim follows from the independence of $\xi_1, \ldots, \xi_r$ in 8. Otherwise, as $f(p\xi_s) \equiv 0 \pmod{p^\ell}$ holds, the element $p\xi_s$ can be written uniquely as $p\xi_s = \alpha_{s+1}\xi_{s+1} + \cdots + \alpha_r \xi_r$ with $\alpha_i \in \{0, \ldots, p-1\}$. Note that the the elements ξ_i, with $s < i \leq r$, have a weight strictly less than ξ_s; i.e. if $w(\xi) = \min\{i \mid p^i \xi \equiv 0 \pmod{[\ldots, p^\ell, \ldots]}\}$ denotes the *weight* of ξ, then, by construction, we have that $w(\alpha_i) \leq w(\xi_s)$. Suppose that $w(\alpha_i) = w(\xi_s)$ holds for some $s < i \leq r$. Then we obtain that

$$\alpha_{s+1}\, p^{a-1}\, \xi_{s+1} + \cdots + \alpha_r\, p^{a-1}\, \xi_r = p^a \xi_s \equiv 0 \pmod{[\ldots, p^\ell, \ldots]}$$

which contradicts the independence of $\xi_{s+1}, \ldots, \xi_r$ of weight p^a if at least one α_i does not vanish. Thus, by induction on the weight, we obtain that Equation (14) implies that $t_1 = u_1, \ldots, t_s = u_s$, and additionally

$$t_i + \delta\alpha_i \equiv u_i + \varepsilon\alpha_i \pmod{p}.$$

By Equation (13), this yields that $\delta = \varepsilon$ and therefore, by the choice of the t_i's and u_i's we finally obtain $t_i = u_i$, for each $1 \leq i < s$ or $s < i \leq r$. □

We summarize the algorithm in 6.3.1. Note that we only used the fact that the linear system arises from an endomorphism of an abelian p-group, in form of the divisibility condition in (6). Clearly, the divisibility condition is always satisfied for any linear system of equations over a homocyclic p-group. Therefore the algorithm HenselLifting also applies to the following problems:

- Let G be an abelian p-group and let $g_1, \ldots, g_n \in G$. Decide whether or not $b \in \langle g_1, \ldots, g_n \rangle$ holds.

Algorithm HENSELLIFTING (A, b, p, $e_1 \leq \ldots \leq e_m$)
  Determine the solutions to $Ax \equiv b \pmod{p}$.
  for $\ell \in \{1, \ldots, e_m\}$ **do**
    Echelonize the sub-matrix $\tilde{A}$ modulo p^ℓ.
    Let $k(\ell) = \min\{i \mid \ell \leq e_i\}$.
    for $n \in \{m, m-1, \ldots, k(\ell)\}$ **do**
      Let α_{jn} be the corner-entry corresponding to x_n.
      if $\alpha_{jn} \not\equiv 0 \pmod{p}$ **then**
        Evaluate Equation (9) and determine $t \in \{0, \ldots, p-1\}$
        Lift the solution x_n uniquely.
      else
        Consider the condition (10).
        if this cannot be satisfied **then**
          return fail;
        else
          Restrict to the solutions in Lemma 6.
          Lift these latter solutions.
        end if;
      end if;
    end for;
  end for;

Algorithm 6.1: Solving endomorphic equations with the Hensel lemma

- Let G be an abelian p-group and let $\varphi: G^m \to G^n$ be a homomorphism. Then the algorithm HENSELLIFTING also solves the linear system of modular equations $Ax = b$, as the divisibility condition is also satisfied in this case.
- Let G be an abelian p-group with generators $g_1, \ldots, g_n$. Further let $\varphi: G \to G$ be an automorphism given by the images $g_1^\varphi, \ldots, g_n^\varphi$. Then the algorithm HENSELLIFTING easily modifies so that it computes the inverse φ^{-1}.

The first problem yields that we can modify the algorithm in Section 6.2 for solving a linear system $x^\varphi = b$ for an arbitrary homomorphism $\varphi: G \to H$ of two abelian p-groups G and H.

6.3.2 Solving linear equations over arbitrary finite p-groups

Let G and H be arbitrary abelian p-groups and let $\varphi: G \to H$ be a homomorphism. The algorithm of Section 6.3.1 generalizes to an algorithm for solving the linear system $x^\varphi = b$ for some $b \in H$. This is a slight modification of the algorithm in Section 6.2.

References

[1] H. U. Besche, B. Eick, and E. A. O'Brien. A millennium project: constructing small groups. *Internat. J. Algebra Comput.*, 12(5):623–644, 2002.

[2] B. Eick. *Algorithms for polycyclic groups.* Habilitationsschrift, Universität Kassel, 2001.

[3] B. Eick and W. Nickel. *Polycyclic - Computation with polycyclic groups*, 2009. A refereed GAP 4 package, see [4].

[4] The GAP Group. GAP – *Groups, Algorithms, and Programming, Version 4.4.12*, 2008.

[5] G. Havas and B. S. Majewski. Integer matrix diagonalization. *J. Symb. Comput.*, 24(3-4):399–408, 1997.

[6] D. F. Holt, B. Eick, and E. A. O'Brien. *Handbook of computational group theory.* Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2005.

[7] F. Lazebnik. *On Systems of Linear Diophantine Equations*, volume 69. The Mathematics Magazine, 1996.

[8] F. Le Gall. Efficient isomorphism testing for a class of group extensions. Preprint!